IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Raymond E. SUORSA et al.	§	Confirmation No.:	9527
Serial No.:	09/838,135	§	Group Art Unit:	2445
Filed:	April 20, 2001	§	Examiner:	T. M. Hossain
For:	Automated Provisioning Of Computer Networks Using A Network Database Data Model	§	Docket No.:	200704494-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: February 27, 2010

Sir:

Appellants hereby submit this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on December 28, 2009.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P. (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment from HPC to HPDC was recorded on May 7, 2008, at Reel/Frame 020909/0707.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-64.
Claim cancellations:	3.
Added claims:	65.
Presently pending claims:	1-2 and 4-65.
Presently appealed claims:	1-2 and 4-65.

IV. STATUS OF THE AMENDMENTS

No claims were amended after the final Office action dated October 29, 2009.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims, referring to the specification by page and line number or to the drawings by reference characters as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified with a corresponding reference to the specification or drawings where applicable. The specification references are made to the application as filed by Appellants. Note that the citation to passages in the specification or drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element. Also note that these specific references are not exclusive; there may be additional support for the subject matter elsewhere in the specification and drawings.

Dissemination of information over the Internet typically involves use of web sites.[1] Each web site requires an infrastructure (e.g., site content storage, web servers, application servers, etc.) at one of more centralized locations connected to the Internet.[2] Each server supporting a web site is provisioned with software necessary for the site.[3] Provisioning includes installation and configuration of operating system and application software necessary for the site, and loading of site content.[4]

In the past, provisioning was often carried out manually.[5] However, manual provisioning is time-consuming and prone to error.[6] To overcome the shortcomings of manual provisioning, various techniques of automatic software deployment have been developed.[7] For example, in an enterprise where all of the users interact with the same legacy applications, a "cookie cutter" type of

---

[1] P. 1, ¶ [0003], lines 1-9.

[2] P. 1-2, ¶ [0003], lines 9-21.

[3] P. 2, ¶ [0005], lines 3-6.

[4] P. 2, ¶ [0005], lines 6-9; p. 3, ¶ [0006], lines 1-11.

[5] P. 3, ¶ [0007], lines 1-2.

[6] P. 3-4, ¶ [0007], lines 3-15.

[7] P. 4, ¶ [0009], lines 1-4.

approach, where every computer has the same set of programs, can be used to deploy the software.[8] Once the programs and settings have been determined, they can be packaged in a fixed format (i.e., a "ghost" or "brick"), and automatically disseminated to all of the appropriate computers.[9]

The cookie cutter approach is not effective in situations where computers need to be customized to accommodate individual requirements of varied users.[10] In a data center housing many different web sites, each site likely uses different business logic requiring different combinations of hardware and software.[11] Appellants have devised agent-based techniques for provisioning computers that overcome the aforementioned deficiencies of the prior art.[12]

The invention of claim 1 is directed to a method for automated provisioning of computer networks. The method includes receiving, by a network device to be provisioned, at least one unsolicited software retrieval command to be executed on the network device.[13] The command is sent by a secure provisioning network 31 connected via a network to the network device.[14] The provisioning network reads parameters of the network device from a network database 32.[15] The reading is responsive to an inquiry based on the at least one command and received from the network device.[16] The provisioning network determines whether the at least one command can be properly executed on the network device based upon the parameters read.[17] The network device executes the at

---

[8] P. 4, ¶ [0009], lines 5-8.

[9] P. 4, ¶ [0009], lines 9-11.

[10] P. 5, ¶ [0010], lines 1-3.

[11] P. 5, ¶ [0010], lines 5-17.

[12] P. 6, ¶[0012], lines 1-9.

[13] Fig. 7, p. 17, ¶ [0049], lines 1-3.

[14] Figs. 6-7; p. 16, ¶ [0047], lines 4-6; p. 18-19, ¶ [0051], lines 14-15.

[15] Fig. 7; p. 16, ¶ [0047], lines 11-19; p. 18, ¶ [0051], lines 7-9.

[16] P. 18, ¶ [0051], lines 4-9.

[17] P. 18, ¶ [0051], lines 7-9.

least one command only if it is determined that the at least one command can be properly executed.[18]

[18] P. 19, ¶ [0051], lines 20-24.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2 and 4-65 are obvious under 35 U.S.C. § 103 over Black (U.S. Pub. No. 2002/0116485, hereinafter "*Black*") in view of Official Notice.

VII. ARGUMENT

A. Rejections Under 35 U.S.C. § 103 Over Black and Official Notice

1. Claim 1

Independent claim 1 requires "receiving, by a network device to be provisioned, at least one unsolicited software retrieval command, sent by a secure provisioning network connected via a network to the network device, to be executed on said network device." The Examiner cited *Black*, ¶¶ [0410]-[0411], [0419]-[0422], and [0110]-[0112] as allegedly teaching these limitations. *Black* is directed to improving management and network availability by providing out-of-band management channels between network/element management system ("NMS") clients and servers.[19]

Black ¶¶ [0410]-[0411] teach use of templates by an Operations Support Services ("OSS") client to perform tasks. Control, provisioning, and batch are three general categories of templates used by the OSS client.[20] "The instructions within a provisioning template cause the OSS client to issue appropriate calls to the NMS server which cause the NMS server to complete the provisioning task, for example, by writing/modifying data within the network device's configuration database."[21]

Black ¶¶ [0419]-[0422] teach interactive operations performed by a network manager via an OSS client to provision a service within a network device. For example, execution of an SPATH template by the OSS client can cause a NMS server to set up a SONET path in a network device.[22]

Black ¶¶ [0110]-[0112] teach that a network administrator uses the NMS to provision devices (e.g., to enable a port of a device, or support protocols and services).

---

[19] *Black*, Abstract.

[20] *Black*, ¶¶ [0410]-[0411].

[21] *Black*, ¶ [0410].

[22] *Black*, ¶ [0420].

The Examiner admitted *Black* fails to teach that the command received by the device to be provisioned is a "software retrieval command."[23] The Examiner contends that *Black* suggests a software retrieval command. The Examiner postulates that use of templates suggests the concept of software retrieval.[24] However, *Black* teaches execution of templates by the OSS client, not by the device being provisioned,[25] and execution of templates on the OSS client has nothing to do with a software retrieval command in a network device being provisioned. Appellants respectfully submit that *Black* fails to suggest such a command. Instead, *Black* teaches provisioning by pushing an NMS database into the device.[26] Such a pushing operation fails to suggest any type of retrieval command received by the network device.

The Examiner further takes Official Notice that "it would have been obvious to per se disclose a specific software retrieval command."[27] Appellants respectfully submit that obviousness is not a condition for which Official notice can be taken, and whether it would have been obvious to disclose something admittedly not disclosed is irrelevant. Therefore, the Examiner erred in his use of Official Notice. If, "it would have been obvious to per se disclose" a software retrieval command is a statement of the Examiner's belief that provisioning by software retrieval command is a fact "capable of instant and unquestionable demonstration as being well-known," then Appellants respectfully disagree and submit that the Examiner has not shown support for his position. Additionally, use of Official Notice "should be rare when an application is under final

---

[23] *Final Office Action*, p. 2.

[24] *Final Office Action*, p. 3.

[25] *Black*, ¶¶ [0410]-[411].

[26] *Black*, ¶¶ [0232], [0237].

[27] *Final Office Action*, p. 3.

rejection."[28] Therefore, Appellants respectfully submit that the Examiner's use of Official Notice is improper.

Claim 1 also requires "reading, by said provisioning network, parameters of said network device from a network database, said reading being responsive to an inquiry based on the at least one command and received from said network device." The Examiner cited *Black*, ¶¶ [0165]-[0167] and [0230]-[0231] as allegedly teaching these limitations.

Black ¶¶ [0165]-[0167] teach a network administrator configuring a device via an NMS client GUI, adding a device to a device list by IP address or DNS name, and device configuration by the operations of Fig. 3g, whereby an administrator selects a network device to configure. An NMS client informs an NMS server of the device to be configured, and the server may retrieve a data structure for the physical aspects of the device from a database in the device.[29]

Black ¶¶ [0230]-[0231] teaches offline configuration of a network device, where device configuration is stored in an external NMS database and later reconciled with actual device configuration when the device is on-line.

None of the cited passages, nor any other passage in *Black* teaches or suggests reading, by the provisioning network, parameters of the network device from a network database, where the reading is responsive to an inquiry based on the at least one command and the inquiry is received from the network device as required by claim 1. Rather, *Black* ¶ [0167] teaches reading a configuration database based on lack of configuration data in a local cache. *Black* ¶ [0231] teaches reconciliation of an NMS database with a device internal database based on notification that a device is to be managed on-line. *Black* neither teaches nor

---

[28] MPEP § 2144.03 A. "It might not be unreasonable for the examiner in a *first* Office action to take official notice of facts by asserting that certain limitations in a *dependent* claim are old and well known expedients in the in the art without the support of documentary evidence provided the facts so noticed are of notorious character and serve only to *"fill in the gaps"* which might exist in the evidentiary showing made by the examiner to support a particular ground of rejection." *Id.* (citing *In re Zurko*, 258 F.3d 1379, 1385 (Fed. Cir. 2001); *In re Ahlert*, 424 F.2d 1088, 1092 (CCPA 1970)) (emphasis added).

[29] *Black*, ¶ [0167].

suggests database access responsive to an inquiry received from the device being provisioned. Furthermore, *Black* fails to teach or even suggest such an inquiry based on a provisioning command received by the device.

Claim 1 further requires "determining, by said provisioning network, whether the at least one command can be properly executed on said network device based upon the parameters read." The Examiner cited *Black* ¶¶ [0236]-[0237] as allegedly teaching these limitations. The cited portion of *Black* teaches checking for conflicts between the NMS database and the device database before pushing the NMS database to the device. However, this conflict check is not a determination of whether a command previously received by the device can be properly executed by the device as claim 1 requires, but rather is a determination of whether the NMS database should be reconciled before being pushed to the device.

Claim 1 further requires "executing the at least one command on said network device only if it is determined that the at least one command can be properly executed." The Examiner again cited *Black* ¶¶ [0236]-[0237] (explained above) as allegedly teaching these limitations. However, the conflict check of *Black* does not teach or suggest that a network device executes a previously received command only if it is later determined that the command can be properly executed as required by claim 1.

For at least these reasons, *Black* fails to teach or even suggest the limitations of independent claim 1. Therefore, Appellants respectfully submit the that Examiner erred in rejecting all pending claims and request that the rejections of the claims 1, 2 and 4-65 be reversed, and the claims set for issue.

2. Claim 2

Claim 2 requires "the at least one command is executed by an agent on said network device, the agent being configured to manipulate all of the software on the network device." The Examiner cited *Black* ¶¶ [0191]-[0193] as allegedly teaching these limitations. The cited portion of *Black* teaches a "SONET path wizard" in conjunction with the GUI displays of Figs. 5a-h provided by the NMS client. The SONET path wizard is executed on the NMS client and is unrelated to

whether an agent on the device being provisioned is configured to manipulate all software on the device as required by claim 2. Appellants are unable to locate any passage in *Black* teaching or even suggesting these limitations. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 2.

3. Claim 6

Claim 6 requires "the step of determining [of claim 1] is based on reading software packaging parameters." The Examiner cited *Black* ¶¶ [0165]-[0167] as allegedly teaching these limitations. The cited portion of *Black* teaches network device configuration, but fails to even mention reading software packaging parameters or that packaging parameters are used to determine whether the command be properly executed on the device. Thus, *Black* fails to teach or even suggest the limitations of claim 6. Appellants are unable to identify any passage in *Black* teaching or even suggesting these limitations. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 6 and all claims depending therefrom.

4. Claim 58

Claim 58 requires "the step of executing the at least one command is limited to entities having an approved access level to execute the at least one command." The Examiner cited *Black* ¶ [0480] as allegedly teaching these limitations. *Black* ¶ [0480] teaches operations involved with changing the configuration database schema. Such conversion has nothing to do with executing a provisioning command or limiting such execution of a software retrieval command to entities having an approved access level. Appellants are unable to identify any passage in *Black* teaching or even suggesting these limitations. Thus, *Black* fails to teach or even suggest the limitations of claim 58. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 58 and all claims depending therefrom.

5. Claim 65

Claim 65 requires "the step of determining [of claim 1] is based upon an identification of a virtual local area network (VLAN) with which said network

device is associated." The Examiner cited *Black* ¶¶ [0165]-[0167], [0431], and [0474] as allegedly teaching these limitations. *Black* ¶¶ [0165]-[0167] are explained above with regard to claim 1. *Black* ¶ [0474] teaches software component signature generation. *Black* ¶ [0431] teaches a BATCH template used to establish a connection between an NMS server and a network device. None of these portions of *Black*, or any other, teach or suggest identifying a VLAN with which a device is associated as part of determining whether the command can be properly executed on the network device. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 65.

B. Conclusion

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/David M. Wilson/

David M. Wilson
PTO Reg. No. 56,790
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
3404 E. Harmony Road
Fort Collins, CO 80528-9599

VIII. CLAIMS APPENDIX

1. A method for automated provisioning of computer networks, comprising the steps of:

receiving, by a network device to be provisioned, at least one unsolicited software retrieval command, sent by a secure provisioning network connected via a network to the network device, to be executed on said network device;

reading, by said provisioning network, parameters of said network device from a network database, said reading being responsive to an inquiry based on the at least one command and received from said network device;

determining, by said provisioning network, whether the at least one command can be properly executed on said network device based upon the parameters read; and

executing the at least one command on said network device only if it is determined that the at least one command can be properly executed.

2. The method of claim 1, wherein the at least one command is executed by an agent on said network device, the agent being configured to manipulate all of the software on the network device.

4. The method of claim 1, further comprising:

verifying the validity of the command by requesting verification from the secure provisioning network.

5. The method of claim 4, wherein the step of verifying is accomplished by way of communicating with a communication gateway of the secure provisioning network.

6. The method of claim 1, wherein the step of determining is based on reading software packaging parameters.

7. The method of claim 6, wherein the software packaging parameters comprise compatibility requirements.

8. The method of claim 6, wherein the software packaging parameters comprise software roles.

9. The method of claim 7, wherein the compatibility requirements comprise software roles compatibility requirements.

10. The method of claim 6, wherein the software packaging parameters comprise operating system (OS) parameters.

11. The method of claim 7, wherein the compatibility requirements comprise operating system (OS) compatibility requirements.

12. The method of claim 6, wherein the software packaging parameters comprise parameters regarding specific customer account requirements.

13. The method of claim 7, wherein the compatibility requirements comprise requirements regarding specific customer account compatibility.

14. The method of claim 8, wherein the software roles comprise customer account software roles.

15. The method of claim 9, wherein the software roles compatibility requirements comprise customer account software roles compatibility requirements.

16. The method of claim 6, wherein the software packaging parameters comprise device parameters.

17. The method of claim 16, wherein the device parameters comprise device interface parameters.

18. The method of claim 17, wherein the device interface parameters comprise device internet protocol (IP) address parameters.

19. The method of claim 17, wherein the interface parameters comprise interface type parameters.

20. The method of claim 16, wherein the device parameters comprise interface components parameters.

21. The method of claim 16, wherein the device parameters comprise memory components parameters.

22. The method of claim 16, wherein the device parameters comprise storage components parameters.

23. The method of claim 16, wherein the device parameters comprise central processing unit (CPU) parameters.

24. The method of claim 7, wherein the compatibility requirements comprise device compatibility requirements.

25. The method of claim 24, wherein the device compatibility requirements comprise interface compatibility requirements.

26. The method of claim 25, wherein the interface compatibility requirements comprise IP compatibility requirements.

27. The method of claim 25, wherein the interface compatibility requirements comprise interface type compatibility requirements.

28. The method of claim 24, wherein the device compatibility requirements comprise interface components compatibility requirements.

29. The method of claim 24, wherein the device compatibility requirements comprise memory components compatibility requirements.

30. The method of claim 24, wherein the device compatibility requirements comprise storage components compatibility requirements.

31. The method of claim 24, wherein the device compatibility requirements comprise central processing unit (CPU) components compatibility requirements.

32. The method of claim 8, wherein software roles compatibility requirements comprise device roles compatibility requirements.

33. The method of claim 9, wherein the software roles comprise device roles.

34. The method of claim 6, wherein the software packaging parameters comprise application packaging parameters.

35. The method of claim 7 wherein the compatibility requirements comprise application compatibility requirements.

36. The method of claim 8, wherein the software roles comprise application software roles.

37. The method of claim 36, wherein the application software roles define a group of services.

38. The method of claim 9, wherein the software roles compatibility requirements comprise application roles compatibility requirements.

39. The method of claim 38, wherein the application roles compatibility requirements define a group of services.

40. The method of claim 6, wherein the software packaging parameters relate to a variety of network service tiers.

41. The method of claim 7, wherein the compatibility requirements are defined according to a variety of network service tiers.

42. The method of claim 6, wherein the software packaging parameters are defined by way of configuration parameters.

43. The method of claim 42, wherein the configuration parameters comprise device configuration parameters.

44. The method of claim 42, wherein the configuration parameters comprise interface configuration parameters.

45. The method of claim 42, wherein the configuration parameters comprise virtual IP address parameters.

46. The method of claim 42, wherein the configuration parameters comprise component type parameters.

47. The method of claim 42, wherein the configuration parameters comprise role configuration parameters.

48. (Original) The method of claim 47, wherein the role configuration parameters comprise device role configuration parameters.

49. (Original) The method of claim 48, wherein the device role configuration parameters comprise device role history configuration parameters.

50. (Original) The method of claim 7, wherein the compatibility requirements comprise configuration compatibility requirements.

51. (Original) The method of claim 50, wherein the configuration compatibility requirements comprise device configuration compatibility requirements.

52. (Original) The method of claim 50, wherein the configuration compatibility requirements comprise interface configuration compatibility, requirements.

53. (Original) The method of claim 50, wherein the configuration compatibility requirements comprise virtual IP address compatibility requirements.

54. (Original) The method of claim 50, wherein the configuration compatibility requirements comprise component type configuration compatibility requirements.

55. (Original) The method of claim 50, wherein the configuration compatibility requirements comprise role configuration compatibility requirements.

56. (Original) The method of claim 55, wherein the role configuration compatibility requirements comprise device role configuration compatibility requirements.

57. (Original) The method of claim 56, wherein the device role configuration compatibility requirements comprise device role history configuration compatibility requirements.

58. (Original) The method of claim 1, wherein the step of executing the at least one command is limited to entities having an approved access level to execute the at least one command.

59. (Original) The method of claim 58, wherein the access to execute the at least one command is defined in an access control list (ACL).

60. (Original) The method of claim 58, wherein the access control list ACL is defined by domain name server (DNS) address of the network device.

61. (Original) The method of claim 58, wherein the entity executing the at least one command comprises an agent.

62. (Original) The method of claim 61 wherein the access to the agent is limited according to domain name server (DNS) address of the network device.

63. (Original) The method of claim 9, wherein the software roles compatibility requirements relate to an IP address of the network device.

64. (Original) The method of claim 9, wherein the software roles compatibility requirements relate to IP address compatibility requirements.

65. (Previously presented) The method of claim 1, wherein the step of determining is based upon an identification of a virtual local area network (VLAN) with which said network device is associated.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.